JOURNAL OF ALGEBRA **71**, 481–489 (1981)

Rational Functions Associated to Presentations of Finite Groups

J. G. THOMPSON

Department of Mathematics, University of Cambridge, Cambridge CB2 1SB, England

Communicated by Walter Feit

Received October 17, 1980

1. NOTATION AND STATEMENTS OF RESULTS

Suppose that F is a free group on generators $x_1,..., x_r$, that $r \geqslant 2$, and that ϕ is a homomorphism of F onto a finite group G of order g. Let S_n be the set of elements x of F of length $l(x) = n$, so that

$$S_0 = \{1\}, \qquad S_1 = \{x_1,..., x_r, x_1^{-1},..., x_r^{-1}\}.$$

Let

$$P(t) = \sum_{\substack{x \in F\\ x \neq 1}} x \cdot t^{l(x)},$$

a formal power series in the indeterminate t. Setting

$$\sigma(S_n) = \sum_{x \in S_n} x \qquad (n \geqslant 0),$$

the coefficient of t^n is $\sigma(S_n)\,(n \geqslant 1)$. The homomorphism ϕ extends to a homomorphism, also denoted ϕ, of the group ring $\mathbb{C}F$ onto the group ring $\mathbb{C}G$, and we set

$$F(t) = \phi(P(t)) = \sum_{\substack{x \in F\\ x \neq 1}} \phi(x) \cdot t^{l(x)}, \tag{1.1}$$

a formal power series in t with coefficients in $\mathbb{C}G$. Thus,

$$F(t) = \sum_{\alpha \in G} F_\alpha(t) \cdot \alpha,$$

0021-8693/81/080481–09$02.00/0

481/71/2-13

where

$$F_\alpha(t) = \sum_{n \geqslant 1} a_n(\alpha) t^n$$

is a power series in t with integral coefficients $a_n(\alpha) = |\phi^{-1}(\alpha) \cap S_n|$.
Set

$$\begin{aligned} \Phi &= \phi(\sigma(S_1)) \\ &= \sum_{i=1}^{r} \{\phi(x_i) + \phi(x_i)^{-1}\}. \end{aligned} \tag{1.2}$$

Let $A = \mathbb{R}[\Phi]$ be the subalgebra of $\mathbb{R}G$ generated by Φ (with 1 adjoined). If $a \in \mathbb{R}G$ and

$$a = \sum_{\alpha \in G} a(\alpha) \cdot \alpha \qquad (a(\alpha) \in \mathbb{R}),$$

then by (1.2)

$$a(\alpha) = a(\alpha^{-1}), \qquad \forall\, \alpha \in G,\ a \in A.$$

In particular, the characteristic roots of Φ are real, since in the right regular representation of $\mathbb{R}G$, Φ is represented by a real symmetric matrix.

Let λ be the linear function of $\mathbb{R}G$ given by $\lambda(a) = a(1)$. Then

$$\lambda(a^2) = \sum_{\alpha \in G} a(\alpha) a(\alpha^{-1}),$$

from which we conclude that

$$0 \neq a \in A \Rightarrow a^2 \neq 0,$$

and so A is semisimple, and of course A is commutative. If $e_1, e_2, \ldots, e_h$ are the primitive idempotents of A, we have

$$1 = \sum_{i=1}^{h} e_i;$$

the characteristic roots of Φ are real, and so $Ae_i = \mathbb{R}e_i$ is one-dimensional and

$$e_i \Phi = \zeta_i e_i, \qquad \zeta_i \in \mathbb{R}.$$

With this notation, we can state

THEOREM 1.

$$F(t)e_i = \frac{\zeta_i t - 2rt^2}{1 - \zeta_i t + (2r-1)t^2}\, e_i.$$

As a consequence of Theorem 1, we get

COROLLARY.

$$F_\alpha(t) = \sum_{i=1}^{h} \frac{\zeta_i t - 2rt^2}{1 - \zeta_i t + (2r-1)t^2} \cdot \lambda(e_i \alpha^{-1}).$$

For $\lambda(e_i\alpha^{-1})$ is the coefficient of α in e_i, and $F(t) = F(t) \cdot 1 = \sum_i F(t)e_i$, so that Theorem 1 yields the Corollary.

So in order to obtain information about $F_\alpha(t)$, we need to understand the ζ_i and the $\lambda(e_i\alpha^{-1})$. The values $\lambda(e_i\alpha^{-1})$ are easy to handle, but the necessary information about the ζ_i is more difficult to find.

Theorem 2 formalizes an intuitively obvious result.

THEOREM 2. *If G has no linear character sg such that $sg(\phi(s)) = -1$ for all $s \in S_1$, then for each $\alpha \in G$,*

$$a_n(\alpha) = \frac{2r(2r-1)^{n-1}}{g} + o((2r-1)^n).$$

If G has a linear character sg such that $sg(\phi(s)) = -1$ for all $s \in S_1$, then for each $\alpha \in G$,

$$a_n(\alpha) = \frac{2r(2r-1)^{n-1}}{g}\{1 + (-1)^n \cdot sg(\alpha)\} + o((2r-1)^n).$$

Remark. Since $\phi(S_1)$ generates G, the character sg is unique when it exists. In addition, in this case $a_n(\alpha) = 0$ if $1 + (-1)^n\, sg(\alpha) = 0$, since $\phi(S_{2n}) \subseteq \ker sg$, $\phi(S_{2n+1}) \cap \ker sg = \varnothing$.

Given Theorem 2, it is natural to try to understand the nature of the small o-functions. I address myself to this in Section 3.

2. THE PROOFS OF THEOREMS 1 AND 2

We work in a commutative subring of $\mathbb{R}F$, namely, the subring

$$L = \sum_{n \geq 0} \mathbb{R}\sigma(S_n).$$

This $\mathbb{R}$-vector space is a ring and is commutative, since, for example,

$$\begin{aligned}\sigma(S_1)\sigma(S_n) &= \sigma(S_n)\sigma(S_1) \\ &= \sigma(S_{n+1}) + (2r-1+\delta_{n,1})\sigma(S_{n-1}), \qquad n=1,2,3,\ldots\end{aligned} \tag{2.1}$$

This relation is obvious, since if $n \geqslant 2$, an element of F of length $n+1$ is uniquely of the shape $y_1 \cdot y_n$ $(y_i \in S_i)$, while an element of S_{n-1} is of this shape in $2r-1$ distinct ways; and 1 is the product of two elements of S_1 in $2r$ ways. From (2.1), we get

$$\begin{aligned}P(t)\cdot\sigma(S_1) &= \sum_{n\geqslant 1} \sigma(S_n)\sigma(S_1)t^n \\ &= \sigma(S_1)^2 t + \sum_{n\geqslant 2} \sigma(S_n)\sigma(S_1)t^n \\ &= (\sigma(S_2)+2r)t + \sum_{n\geqslant 2} \{\sigma(S_{n+1}) + (2r-1)\sigma(S_{n-1})\}t^n.\end{aligned}$$

Hence,

$$tP(t)\sigma(S_1) = 2rt^2 + \sum_{n\geqslant 2} \sigma(S_n)t^n + \sum_{n\geqslant 2} (2r-1)\sigma(S_{n-1})t^{n+1},$$

whence

$$tP(t)\sigma(S_1) = 2rt^2 + P(t) - \sigma(S_1)t + (2r-1)\,t^2P(t). \tag{2.2}$$

If we apply ϕ to (2.2) and take account of (1.2) and (1.1), we find that

$$(1+(2r-1)t^2)\,F(t) - tF(t)\Phi - t\Phi + 2rt^2 = 0. \tag{2.3}$$

If e is a primitive idempotent of A, then $e\Phi = \zeta e$, and if we multiply (2.3) by e, we get

$$\{1+(2r-1)t^2 - \zeta t\}\,F(t)e + (2rt^2 - \zeta t) = 0;$$

Theorem 1 follows immediately.

In order to prove Theorem 2, we require only superficial knowledge of the characteristic roots ζ of Φ. Since Φ is a sum of $2r$ group elements, it follows that $2r$ is an upper bound for the absolute value of ζ. If $0 \neq x \in \mathbb{R}G$ satisfies $x\Phi = 2rx$, then x is a multiple of

$$e(1) = (1/g)\,\Sigma\alpha,$$

while if $x\Phi = -2rx$, then x is a multiple of

$$e(sg) = (1/g)\, \Sigma sg(\alpha)\alpha.$$

Apart from these two eigenspaces $\mathbb{R}e(1)$ and $\mathbb{R}e(sg)$, all other eigenvalues ζ satisfy

$$|\zeta| < 2r.$$

It is straightforward to check that if ζ is a real number, $|\zeta| < 2r$, and σ is a root of $1 - \zeta t + (2r-1)t^2$, then

$$|\sigma^{-1}| < 2r - 1. \tag{2.3}$$

With these remarks, we see that Theorem 2 is a consequence of the properties of the partial fraction decomposition of

$$Q_\zeta(t) = \frac{t\zeta - 2rt^2}{1 - \zeta t + (2r-1)t^2}.$$

Indeed

$$Q_{2r}(t) = \frac{2rt}{1-(2r-1)t} = \sum_{n \geqslant 1} 2r(2r-1)^{n-1}t^n,$$

$$Q_{-2r}(t) = \frac{-2rt}{1+(2r-1)t} = \sum_{n \geqslant 1} (-1)^n\, 2r(2r-1)^{n-1}t^n.$$

So suppose $|\zeta| < 2r$. If $\zeta^2 = 4(2r-1)$, then

$$Q_\zeta(t) = \frac{t\zeta - 2rt^2}{(1-\sigma^{-1}t)^2}$$

$$= (t\zeta - 2rt^2) \sum_{n \geqslant 1} n\sigma^{-n}t^{n-1},$$

and as $|\sigma^{-1}| = (2r-1)^{1/2}$, we get

$$q_{\zeta,n} = o(n(2r-1)^{n/2}) = o((2r-1)^n),$$

where $Q_\zeta(t) = \sum_{n \geqslant 1} q_{\zeta,n}t^n$.

If $\zeta^2 \neq 4(2n-1)$, then the denominator of Q_ζ has distinct roots σ, τ, and

$$Q_\zeta(t) = \frac{t\zeta - 2rt^2}{(1-\sigma^{-1}t)(1-\tau^{-1}t)},$$

whence, by (2.3),

$$q_{\zeta,n} = o((2r-1)^n)$$

and Theorem 2 follows.

3. Further Relations

In order to obtain explicit constants for the required estimates of $a_n(\alpha)$, we refine $F(t)e_i$ to take account of the primitive central idempotents of $\mathbb{C}G$. If χ is an irreducible character of G,

$$e(\chi) = \frac{\chi(1)}{g} \sum_{\alpha \in G} \chi(\alpha^{-1})\alpha$$

is the corresponding central idempotent, and

$$F(t)e_i = \sum_{\chi} F(t)e_i e(\chi).$$

I assert that

$$\lambda(e_i e(\chi)) = \frac{\chi(1)}{g} m(i, \chi), \tag{3.1}$$

where the $m(i, \chi)$ are integers $\geqslant 0$ such that

$$\sum_{i=1}^{h} m(i, \chi) = \chi(1). \tag{3.2}$$

Namely, I define $m(i, \chi)$ by

$$\chi(e_i e(\chi)) = m(i, \chi).$$

Then $m(i, \chi)$ is the rank of the idempotent $e_i e(\chi)$ in the $\chi(1) \times \chi(1)$ matrix algebra $\mathbb{C}G \cdot e(\chi)$.

Let

$$e_i e(\chi) = \sum_{\alpha \in G} b(\alpha)\alpha.$$

Then

$$\chi(e_i e(\chi)) = \sum_{\alpha} b(\alpha)\chi(\alpha).$$

Also, of course,

$$\lambda(e_i e(\chi)) = b(1),$$

so (3.1) is the assertion that

$$b(1) = \left\{ \sum_{\alpha \in G} b(\alpha)\chi(\alpha) \right\} \frac{\chi(1)}{g}. \tag{3.3}$$

Now $e_i e(\chi) \cdot e(\chi) = e_i e(\chi)$, and as

$$e_i e(\chi) \cdot e(\chi) = \left\{ \sum_{\alpha} b(\alpha)\alpha \right\} \left\{ \sum_{\beta} \frac{\chi(1)}{g} \chi(\beta^{-1})\beta \right\},$$

(3.3) follows. The idempotents $e_i e(\chi)$ $(1 \leqslant i \leqslant h)$ form an orthogonal decomposition of $e(\chi)$, so (3.2) also holds.

Next, we have

$$e_i = \sum_{\alpha} a(\alpha)\alpha$$

for real numbers $a(\alpha)$ such that $a(\alpha) = a(\alpha^{-1})$. Thus

$$e_i e(\chi) = \left\{ \sum_{\alpha} a(\alpha)\alpha \right\} \left\{ \sum_{\beta} \frac{\chi(1)}{g} \chi(\beta^{-1})\beta \right\},$$

which implies that

$$b(\alpha^{-1}) = \overline{b(\alpha)}.$$

Since $\Sigma b(\alpha)\alpha = e_i e(\chi)$ is an idempotent, we have

$$b(1) = \sum_{\alpha \in G} b(\alpha)\, \overline{b(\alpha)},$$

and since

$$b(\alpha) = \sum_{\xi} b(\xi)\, b(\xi^{-1}\alpha),$$

Schwartz's inequality implies that

$$|b(\alpha)| \leqslant b(1). \tag{3.4}$$

Or, in another notation,

$$|\lambda(e_i e(\chi)\alpha^{-1})| \leqslant \frac{\chi(1)}{g} m(i, \chi). \tag{3.5}$$

From now on, we reserve the symbol sg to denote the linear character of G in Theorem 2, when it exists, and let χ be an irreducible character of G distinct from sg and from the principal character. Let $I(\chi)$ be the set of non-zero idempotents of the shape $e_i e(\chi)$ $(1 \leqslant i \leqslant h)$, and let $C(\chi)$ be the set of characteristic roots of Φ associated to the members of $I(\chi)$. Let

$$\begin{aligned} \mu &= \mu(\Phi, \chi) \\ &= \max |\sigma^{-1}|, \end{aligned}$$

where σ ranges over the roots of $1 - \zeta t + (2r-1)t^2$, and ζ ranges over $C(\chi)$. By a previous remark,

$$\mu < 2r - 1.$$

Now we have

$$F_\alpha(t) = \sum_\chi F_{\alpha,\chi}(t),$$

$$\begin{aligned} F_{\alpha,\chi}(t) &= \sum_{e \in I(\chi)} \frac{\zeta t - 2rt^2}{1 - \zeta t + (2r-1)t^2} \cdot \lambda(e\alpha^{-1}) \\ &= \sum_{n \geqslant 1} a_{n,\chi}(\alpha) t^n. \end{aligned}$$

To avoid notation difficulties, I assume that the roots σ, τ of $1 - \zeta t + (2r-1)t^2$ are distinct for each relevant ζ. Then

$$\begin{aligned} \frac{\zeta t - 2rt^2}{1 - \zeta t + (2r-1)t^2} = \sum_{n \geqslant 0} \Bigg\{ &-2r(2r-1)\left(\frac{\sigma^{-n} - \tau^{-n}}{\sigma^{-1} - \tau^{-1}}\right) \\ &+ \zeta \cdot (2r-1)\left(\frac{\sigma^{-n-1} - \tau^{-n-1}}{\sigma^{-1} - \tau^{-1}}\right)\Bigg\} t^{n+1}, \end{aligned}$$

and so, for $n \geqslant 0$, $\alpha \in G$, we have

$$\begin{aligned} a_{n+1,\chi}(\alpha) = \sum_{e \in I(\chi)} \Bigg\{ &-2r(2r-1)\left(\frac{\sigma^{-n} - \tau^{-n}}{\sigma^{-1} - \tau^{-1}}\right) \\ &+ \zeta \cdot (2r-1)\left(\frac{\sigma^{-n-1} - \tau^{-n-1}}{\sigma^{-1} - \tau^{-1}}\right)\Bigg\} \cdot \lambda(e\alpha^{-1}). \end{aligned}$$

From the definition of $\mu = \mu(\Phi, \chi)$, and from (3.1), (3.3), (3.4) we have

$$|a_{n+1,\chi}(\alpha)| \leqslant \sum_{e \in I(\chi)} \{2r(2r-1)\mu^{n-1} \cdot n + 2r(2r-1)\mu^n(n+1)\} \cdot \frac{\chi(1)}{g} \cdot m(i, \chi).$$

Thus, (3.2) implies that

$$|a_{n,x}(\alpha)| \leqslant \frac{\chi(1)^2}{g} 4r(2r-1)(n+1)\mu^{n-1}.$$

Summing over $\chi \neq 1$, sg, we get

$$\left| a_n(\alpha) - \frac{2r(2r-1)^{n-1}}{g} \right| \leqslant 4r(2r-1)(n+1)M^{n-1},$$

$$M = \max_{\chi \neq 1} \{\mu\},$$

if sg does not exist, and

$$\left| a_n(\alpha) - \frac{2r(2r-1)^{n-1}}{g} (1 + (-1)^n\, sg(\alpha)) \right| \leqslant 4r(2r-1)(n+1)M^{n-1},$$

$$M = \max_{\chi \neq 1, sg} \{\mu\},$$

if sg exists.

This discussion only underscores the relevance of the characteristic roots of Φ. It seems particularly interesting to me to determine which of these ζ satisfy $|\zeta| < 2(2r-1)^{1/2}$, since in this case, the roots of $1 - \zeta t + (2r-1)t^2$ are complex, each of absolute value $(2r-1)^{-1/2}$. Thus, in the case when all ζ are either $\pm 2r$ or at most $2(2r-1)^{1/2}$ in absolute value, the $o((2r-1)^n)$ in Theorem 2 can be replaced by $O(n(2r-1)^{n/2})$, a more satisfying state of affairs and which, I suspect, captures the truth for many presentations.

The ideas in this paper go back to my student days. I was stimulated to write down my musings by the Hungarian cube, which appears to have an associated presentation such that for a remarkably small N, $a_n(\alpha) + a_{n+1}(\alpha) \neq 0$ for all α and all $n \geqslant N$. Presumably, this is accounted for by the fact that if $\mu = \mu(\Phi, \chi)$ is close to $2r-1$, then $\chi(1)$ is small, so that the "damping" factor $\chi(1)^2/g$ which appears in the estimate for $a_{n,x}(\alpha)$ produces a small N.

One could replace the free group F by the free product of finite cyclic groups, and obtain similar generating functions. No new idea is involved.